CHAOS BASED IMAGE ENCRYPTION

(Report For Numerical Methods and Programming, Spring 2023)

Kasi Viswanath (18414) and Siddhant Aggarwal (18263)

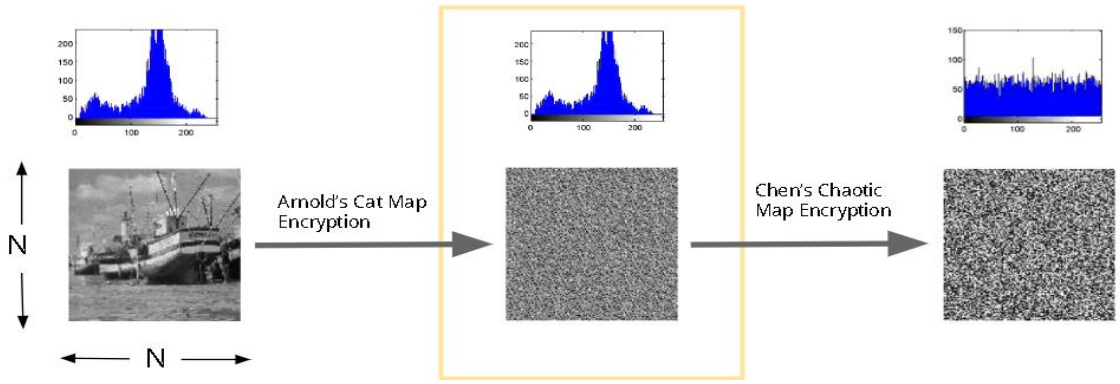
Indian Institute of Science Education and Research, Bhopal

Introduction

Image encryption is a crucial technique used to secure digital images from unauthorised access. A new image encryption scheme has been presented by Guan et al. in their paper “Chaos-based image encryption algorithm” published in Physics Letters A in 2005. The proposed scheme uses the combination of shuffling the positions and changing the grey values of image pixels to confuse the relationship between the cipher-image and the plain-image. In this report, we will provide an overview of the proposed encryption scheme and its experimental results.

Encryption Scheme

The proposed encryption scheme is a two-stage process. In the first stage, the Arnold cat map is used to shuffle the positions of the image pixels in the spatial domain. The Arnold cat map is a chaotic map that has been widely used in image encryption due to its high sensitivity to initial conditions and parameters. The Arnold cat map iteratively rearranges the positions of the pixels in an image, resulting in a shuffled image.



In the second stage, the discrete output signal of Chen's chaotic system is pre-processed to be suitable for grayscale image encryption, and the shuffled image is encrypted by the pre-processed signal pixel by pixel. Chen's chaotic system is a three-dimensional autonomous chaotic system that has been found to be useful in cryptography. The discrete output signal of Chen's chaotic system is used to change the grey values of the pixels in the shuffled image.

Arnold Cat Map

The Arnold Cat map is a discrete-time dynamical system that shuffles the positions of the image pixels in the spatial-domain. The map is defined as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \pmod N = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N$$

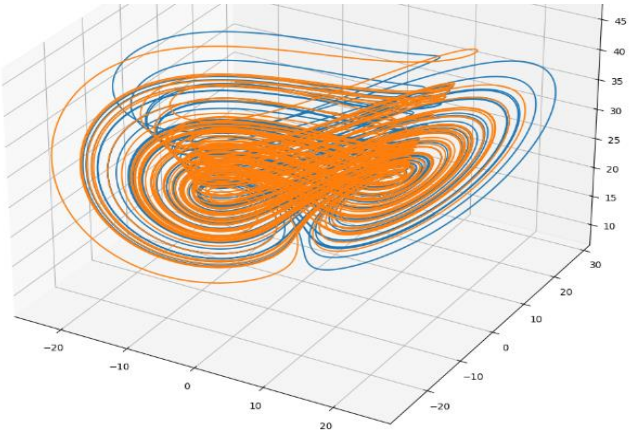
p and *q* are positive integers, det(A)=1. The map is area-preserving since the determinant of its linear transformation matrix equals. The (x',y') is the new position of the original pixel position (x,y) when Arnold cat map is performed once. The Arnold Cat map is a popular choice for image scrambling due to its ability to generate complex and unpredictable patterns.

Chen's Chaotic System

Chen's chaotic system is a continuous-time dynamical system that is used to generate a pseudorandom signal for grayscale image encryption. The system is described by the following equations:

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = (c - a)x - xz + cy, \\ \dot{z} = xy - bz, \end{cases}$$

where x, y, and z are the state variables, t is time, and a, b, and c are constants. Chen's chaotic system exhibits chaotic behaviour, which means that small changes in the initial conditions can lead to large changes in the output signal. This property makes it suitable for use in cryptographic applications.



The output signal of Chen's chaotic system is discretized and used to encrypt the shuffled image pixel by pixel. The resulting cipher-image is highly scrambled and appears random-like, which makes it difficult for attackers to recover the original image without the correct decryption key.

Pre-Processing

The Chen's chaotic system is iterated continuously. For each iteration, we can get three values xi, yi and zi. These decimal values are pre-processed first as follows:

$$B_{x_i} = \mathrm{de2bi}\left(\mathrm{mod}\left(\left(\mathrm{Abs}(x_i) - \mathrm{Floor}\left(\mathrm{Abs}(x_i)\right)\right) 10^{14}, 256\right)\right),$$

where Abs(xi) returns the absolute value of *x*. Floor(x) rounds the elements of *x* to the nearest integers less than or equal to *x*. mod(x,y) returns the remainder after division. The function de2bi(x) converts decimal number *x* to binary value. The decimal fractions of the variables are multiplied by 10^{14}. Moreover, in mod(x,,y) function the variable *y* is chosen as 256 because the grayscale image with 256 grey levels.

Encryption

The encryption is performed by operation Exclusive OR (XOR) between the pixel gray value and the modified chaos system's Bx, By, Bz values.

$$C_{3\times(i-1)+1} = B_{3\times(i-1)+1} \oplus B_{x_i},$$
$$C_{3\times(i-1)+2} = B_{3\times(i-1)+2} \oplus B_{y_i},$$
$$C_{3\times(i-1)+3} = B_{3\times(i-1)+3} \oplus B_{z_i},$$

The XOR operation is a binary operation that outputs a 1 only when the two input bits are different, and a 0 when they are the same. By applying this operation to the pixel and key values, the resulting encrypted image becomes incomprehensible to anyone who does not have the correct key values.

Experimental Results

The proposed encryption scheme was tested on various standard test images, including Lena, Baboon, and Boat. The experimental results showed that the key space of the proposed scheme is large enough to resist brute-force attacks. The distribution of grey values of the encrypted image was found to have a random-like

behaviour, which is essential for secure image encryption. The results, visualization and analysis are in the attached python notebook.

Security Analysis

The encryption algorithm, the initial values of Chen's chaotic system are used as secret keys. If the precision is 10^{-14}, the key space size is 10^{42}. Moreover, the parameters p, q and M of Arnold cat map are also used as the secret keys. The key space is large enough to resist all kinds of brute-force attacks. The experimental results also demonstrate that the scheme is very sensitive to the secret key mismatch (10^{-14}). The experiments for security analysis are shown in the python notebook.

Conclusion

In conclusion, the proposed image encryption scheme is a secure and efficient method for protecting digital images from unauthorized access. The combination of the Arnold cat map and Chen's chaotic system ensures a high degree of randomness and complexity, making it difficult for attackers to decipher the encrypted image. The experimental results demonstrate the effectiveness of the proposed scheme in providing secure image encryption.

Future Directions

There is always room for improvement in any cryptographic algorithm, and the proposed encryption scheme is no exception. One potential area for future research is to explore the possibility of using multiple chaotic systems to improve the security of the encryption scheme further. Additionally, the proposed scheme can be extended to video and audio encryption, which would be an interesting area of research.

Overall, the proposed encryption scheme is a significant contribution to the field of image encryption and provides a secure and efficient method for protecting digital images from unauthorized access. The experimental results demonstrate the effectiveness of the proposed scheme in providing secure image encryption, and the potential for future research is promising.

References

[1] Z. Guan, F. Huang, W. Guan; ‘Chaos-based image encryption algorithm’; Physics Letters A, Volume 346, Issues 1–3, 2005, Pages 153-157.